IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF TEXAS

MARSHALL DIVISION

NO MAGIC, INC.,	§	
	§	
Plaintiff,	§	
	§	CIVIL ACTION NO. 2:17-cv-282
v.	§	
	§	
ATOS IT SOLUTIONS AND SERVICES, INC. and BULL HN INFORMATION SYSTEMS, INC.,	§	**JURY TRIAL DEMANDED**
	§	
	§	
	§	
Defendants.	§	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff No Magic, Inc. files this Complaint against Atos IT Solutions and Services, Inc. and Bull HN Information Systems, Inc. for infringement of United States Patent No. 8,929,552 (the "'552 Patent").

I. NATURE OF THE ACTION

1. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 271, *et seq.*, to enjoin and obtain damages resulting from Defendants' unauthorized use, sale, and offer to sell in the United States of products, methods, processes, services and/or systems that infringe Plaintiff No Magic, Inc.'s United States patent, as described herein.

II. PARTIES

2. Plaintiff No Magic, Inc. ("No Magic" or "Plaintiff") is a corporation organized and existing under the laws of the State of Wyoming, with its principal place of business located at One Allen Center, 700 Central Expressway South, Suite 110, Allen, Texas 75013.

3. No Magic is a twenty-one-year-old company whose primary focus is on the development of software products and solutions for a wide variety of customers. With over 10,000 customer companies, No Magic offers award-winning software products and services to a wide variety of industries, including the energy, automotive, financial, logistics, telecommunications and space exploration (NASA) industries.

4. On information and belief, Defendant Atos IT Solutions and Services, Inc. (“Atos”) is a Delaware corporation with a North American headquarters at 2500 Westchester Avenue, Suite 300, Purchase, New York 10577 and a Dallas regional headquarters at 4851 Regent Boulevard, Irving, Texas 75063. Atos’ registered agent for service of process in Delaware is Corporation Service Company, 2711 Centerville Road, Suite 400, Wilmington, Delaware 19808.

5. On information and belief, Defendant Bull HN Information Systems, Inc. (“Bull” or collectively with Atos “Defendants”) is a Delaware corporation with a United States head office at 285 Billerica Road, Chelmsford, Massachusetts 01824. Bull’s registered agent for service of process in Delaware is The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware 19801.

III. JURISDICTION AND VENUE

6. This is an action for patent infringement which arises under the Patent Laws of the United States, in particular, 35 U.S.C. §§ 271, 281, 283, 284 and 285.

7. This Court has exclusive jurisdiction over the subject matter of this action under 28 U.S.C. §§ 1331 and 1338(a).

8. This Court has personal jurisdiction over Defendants, and venue is proper in this Court pursuant to 28 U.S.C. §§1391(b), (c), and 1400.

IV. PLAINTIFF'S PATENT

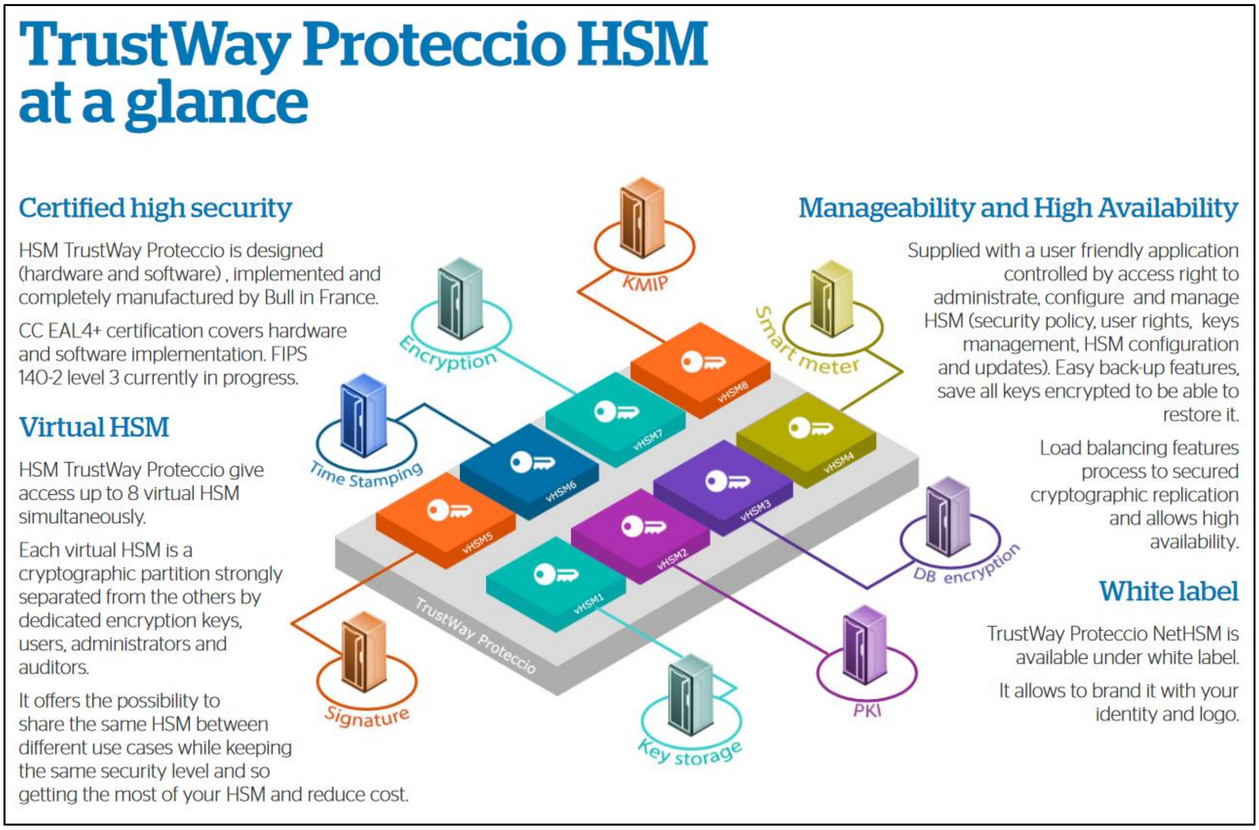
9. The '552 Patent, entitled "Electronic Information and Cryptographic Key Management System" issued on January 6, 2015. At a high level, the '552 Patent discloses systems and methods for the securement of electronic information. The information that is to be secured is associated with a cryptographic key. The key is then secured by encrypting it, saving it, restricting access to it, or by other means. A key management system may be tasked with securing the key and confirming that the key is indeed secured. Once it is confirmed that the key is secured, a function is triggered that is responsible for, for example, enabling the encryption of electronic information, enabling the decryption of electronic information, enabling the transfer of electronic information, enabling the saving of electronic information, enabling electronic information to be read, enabling electronic information to be rewritten, enabling electronic information to be created, enabling electronic information to be manipulated. The '552 Patent discloses enhanced security measures such as using secure socket layer for transferring keys or information and requiring multiple simultaneous access requests from multiple administrators in order to allow access to secure electronic information. A true and correct copy of the '552 Patent is attached as **Exhibit A**.

10. No Magic is the current assignee of the '552 Patent, and has all rights to sue for infringement and collect past and future damages for the infringement thereof.

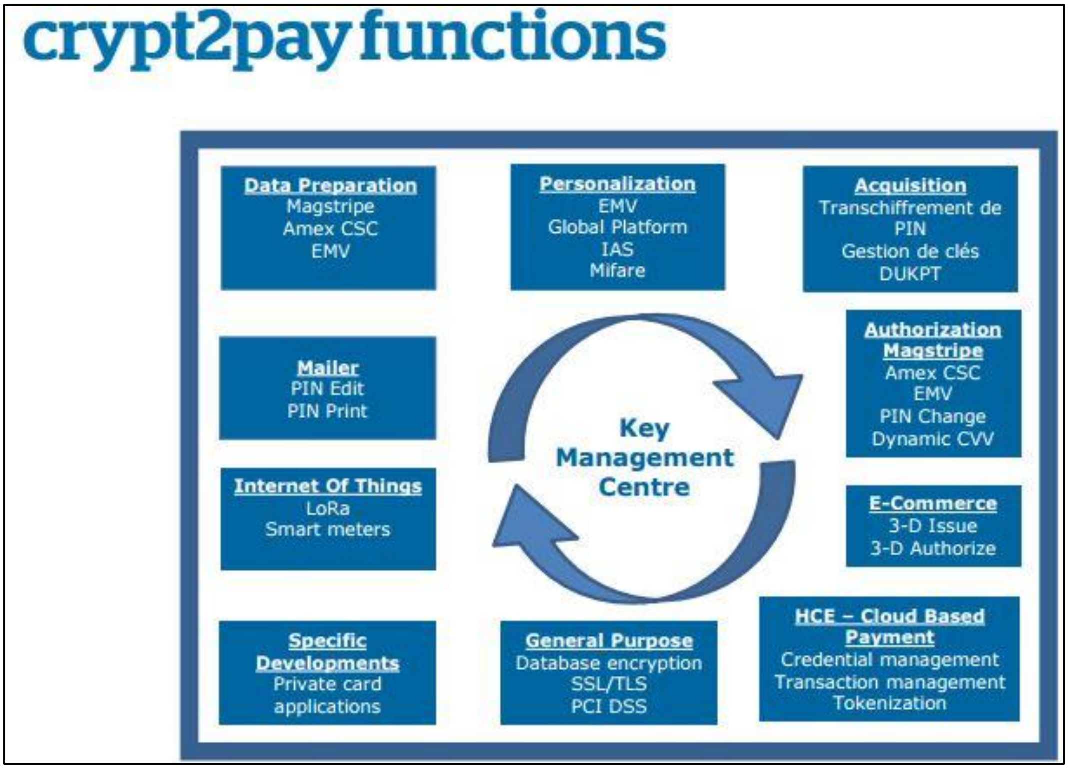
V. DEFENDANTS' ACTS

11. Defendants provides hardware, software, and services that secure electronic information via hardware security modules ("HSMs") and cryptographic operations. For example, the Defendants' TrustWay Proteccio HSM family, comprised of TrustWay Proteccio NetHSM and TrustWay Proteccio OEM-HSM, and Crypt2pay and Crypt2Protect HSMs, along with the Bull Key Management Center ("KMC"), provide secure cryptographic storage,

cryptographic acceleration, administrative access control, and policy management. Defendants' accused products associate a cryptographic key with secured information. This cryptographic key is further secured by encryption or other means. Once the securement of the cryptographic key is confirmed, the accused products enable subsequent cryptographic or data processing functions. The high-level functions of Defendants' Crypt2Pay HSM and TrustWay Proteccio family is illustrated in the images below:


TrustWay Proteccio HSM at a glance
Certified high security
HSM TrustWay Proteccio is designed (hardware and software), implemented and completely manufactured by Bull in France.
CC EAL4+ certification covers hardware and software implementation. FIPS 140-2 level 3 currently in progress.
Virtual HSM
HSM TrustWay Proteccio give access up to 8 virtual HSM simultaneously.
Each virtual HSM is a cryptographic partition strongly separated from the others by dedicated encryption keys, users, administrators and auditors.
It offers the possibility to share the same HSM between different use cases while keeping the same security level and so getting the most of your HSM and reduce cost.
Manageability and High Availability
Supplied with a user friendly application controlled by access right to administrate, configure and manage HSM (security policy, user rights, keys management, HSM configuration and updates). Easy back-up features, save all keys encrypted to be able to restore it.
Load balancing features process to secured cryptographic replication and allows high availability.
White label
TrustWay Proteccio NetHSM is available under white label.
It allows to brand it with your identity and logo.
KMIP
Encryption
Smart meter
Time Stamping
DB encryption
Signature
Key storage
PKI
TrustWay Proteccio
vHSM1
vHSM2
vHSM3
vHSM4
vHSM5
vHSM6
vHSM7
vHSM8

https://bull.com/wp-content/uploads/2016/08/f-proteccio_nethsm-en2_web.pdf


crypt2pay functions
Data Preparation
Magstripe
Amex CSC
EMV
Personalization
EMV
Global Platform
IAS
Mifare
Acquisition
Transchiffrement de PIN
Gestion de clés
DUKPT
Mailer
PIN Edit
PIN Print
Key Management Centre
Authorization Magstripe
Amex CSC
EMV
PIN Change
Dynamic CVV
Internet Of Things
LoRa
Smart meters
E-Commerce
3-D Issue
3-D Authorize
Specific Developments
Private card applications
General Purpose
Database encryption
SSL/TLS
PCI DSS
HCE – Cloud Based Payment
Credential management
Transaction management
Tokenization

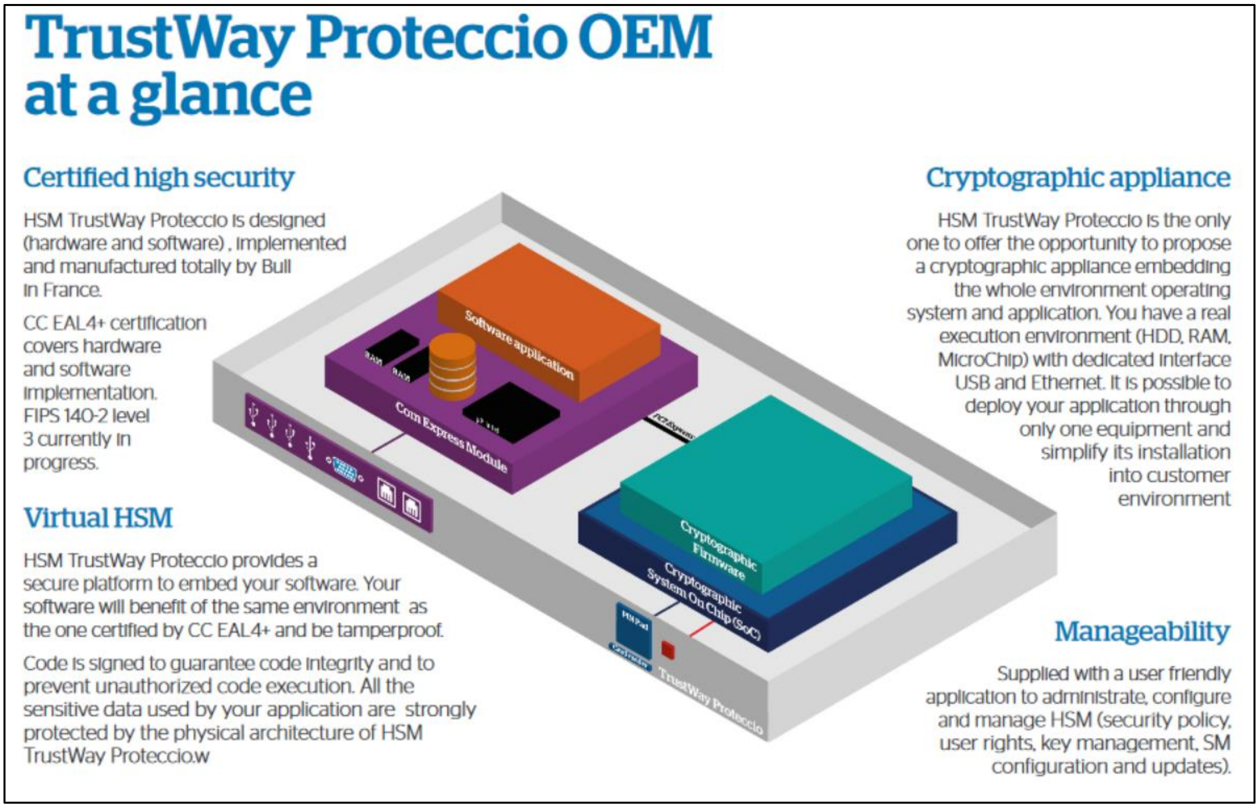
https://bull.com/wp-content/uploads/2016/08/f-crypt2pay-en6_web2.pdf.

12. On information and belief, Defendants also implement contractual protections in the form of license agreements with their customers to preclude the unauthorized reproduction, distribution and modification of their software. Moreover, on information and belief, Defendants implement technical precautions to attempt to thwart customers who would circumvent the intended operation of Defendants' products.

13. Moreover, Defendants provide their customers with the accused products and software and instruct their customers to use the products and software in an infringing manner, including through their website at https://bull.com/hardware-security-module-hsm/, https://bull.com/hsm-trustway-proteccio-nethsm/, and https://bull.com/crypt2pay-hsm-cryptographique/.

14. In addition, Defendants knowingly, actively induced and continue to knowingly, actively induce (or are willfully blind to the) infringement of the '552 Patent within this District

by making, using, offering for sale, and selling infringing products, as well as by contracting with others to use, market, sell, and offer to sell infringing products, all with knowledge of the ’552 Patent, and its claims, with knowledge that their customers will use, market, sell, and offer to sell infringing products in this District and elsewhere in the United States, and with the knowledge and specific intent to encourage and facilitate infringing sales and use of the products by others within this District and the United States by creating and disseminating promotional and marketing materials, instructional materials, product manuals, and technical materials related to the infringing products. Defendants instruct their customers or users to configure, set up, and install the accused products such that they operate in an infringing manner. As seen from the description below, Defendants instruct users to deploy the accused products in a role where it will function to provide a method of securing electronic information and a key management system. Defendants generally describe the infringing functionality in the excerpts below, which can be found in Defendants instructional materials:



TrustWay Proteccio OEM at a glance

Certified high security

HSM TrustWay Proteccio is designed (hardware and software) , implemented and manufactured totally by Bull in France.

CC EAL4+ certification covers hardware and software implementation. FIPS 140-2 level 3 currently in progress.

Cryptographic appliance

HSM TrustWay Proteccio is the only one to offer the opportunity to propose a cryptographic appliance embedding the whole environment operating system and application. You have a real execution environment (HDD, RAM, MicroChip) with dedicated interface USB and Ethernet. It is possible to deploy your application through only one equipment and simplify its installation into customer environment

Virtual HSM

HSM TrustWay Proteccio provides a secure platform to embed your software. Your software will benefit of the same environment as the one certified by CC EAL4+ and be tamperproof.

Code is signed to guarantee code integrity and to prevent unauthorized code execution. All the sensitive data used by your application are strongly protected by the physical architecture of HSM TrustWay Proteccio.w

Manageability

Supplied with a user friendly application to administrate, configure and manage HSM (security policy, user rights, key management, SM configuration and updates).

https://bull.com/wp-content/uploads/2016/08/f-proteccio_oem-en2_web_0.pdf

2.1. Functional Overview

The C2P HR is a multi-chip embedded hardware cryptographic module in the form of an appliance. The appliance contains different electronic components with among them a secure enclosure that provides physical resistance to tampering. The cryptographic boundary of the module is defined to encompass all components inside the secure enclosure.

The C2P HR module is designed to provide secure key generation for symmetric keys and asymmetric key pairs along with symmetric and asymmetric cryptographic services implementing specific algorithms for the banking sector and payment systems.

The C2P HR may concurrently host up to 16 sessions that can be cryptographically separated and presented as "virtual C2P HR boxes" to user applications. Each virtual box provides cryptographic services for user applications and is accessible through a proprietary command interface, communicating with the application server through a TCP/IP connection.

The TCP/IP communication between the C2P HR and an application server, used to perform cryptographic services, may be cryptographically protected using server SSL authentication. It is a requirement when the C2P HR is accessed from a distant network.
The TCP/IP communication between the C2P HR and an administration station, used to perform sensitive administration services, is cryptographically protected using server SSL authentication.

Accesses to virtual tokens may be performed either as authenticated or as unauthenticated, depending on the access control security policy set for the C2P HR. When authentication is being activated, it can be performed either using an identifier with a password or using client SSL authentication.

Crypt2Pay/Crypt2Protect HR Security Policy, v1.2, at 9 (July 4, 2014).

15. Moreover, Defendants knowingly contributed to the infringement of the ’552 Patent by others in this District, and continue to contribute to the infringement of ’552 Patent by others in this District by selling or offering to sell components of infringing products in this District, which components constitute a material part of the inventions of the ’552 Patent, knowing of the ’552 Patent and its claims, knowing those components to be especially made or especially adapted for use to infringe the ’552 Patent, and knowing that those components are not staple articles or commodities of commerce suitable for substantial non-infringing use. The accused products are not staple articles or commodities of commerce because they are specifically designed to perform the claimed functionality. Any other use of the accused products would be unusual far-fetched, illusory, impractical, occasional, aberrant, or experimental.

Defendants have not implemented a design around or otherwise taken any remedial action with respect to the ’552 Patent. No Magic will rely on a reasonable opportunity for discovery of evidentiary information regarding additional infringing products.

VI. COUNT ONE

INFRINGEMENT OF U.S. PATENT NO. 8,929,552

16. Plaintiff No Magic realleges and incorporates herein paragraphs 1–15.

17. No Magic is the assignee and owner of all right, title and interest to the ’552 Patent. No Magic has the legal right to enforce the patent, sue for infringement, and seek equitable relief and damages.

18. The ’552 Patent is valid, enforceable and was duly issued in full compliance with Title 35 of the United States Code.

DIRECT INFRINGEMENT (35 U.S.C. § 271(a))

19. Defendants have directly infringed, and continue to directly infringe, one or more claims of the ’552 Patent in this judicial District and elsewhere in Texas and the United States.

20. Defendants have directly infringed, and continue to directly infringe the ’552 Patent, including but not limited to at least one or more of Claim 1, Claim 4, Claim 16, Claim 17, and claims dependent therefrom, by, among other things, making, using, offering for sale, selling, and/or importing, hardware security modules that secure electronic information and its associated cryptographic keys. Such devices include, but are not limited to, Crypt2Pay HSM, Crypt2Protect HSM, HSM Trustway Proteccio series HSMs, and all reasonably similar products of Defendants.

INDIRECT INFRINGEMENT (INDUCEMENT - 35 U.S.C. § 271(b))

21. Based on the information presently available to No Magic, No Magic contends that Defendants have indirectly infringed, and continue to indirectly infringe, one or more claims

of the ’552 Patent by inducing direct infringement by third parties, including without limitation manufacturers, resellers, and/or end users of the products accused of infringing the ’552 Patent, in this District and elsewhere in the United States.

22. On information and belief, despite having knowledge of the ’552 Patent, Defendants have specifically intended for persons who acquire and use the accused products, including without limitation end-users of the accused products, to acquire and use such devices in such a way that infringes the ’552 Patent, including but not limited to at least one or more of Claim 1, Claim 4, Claim 16, Claim 17, and one or more dependent claims, and Defendants knew or should have known that their actions were inducing infringement.

23. Defendants have had knowledge of the ’552 Patent and the infringing nature of their activities at least as early as the date when No Magic effected service of this Complaint.

24. Direct infringement is the result of activities performed by third parties in relation to the accused products, including without limitation by end users enabled and encouraged by Defendants to use the accused products in their normal, customary way to infringe the ’552 Patent.

25. With knowledge of the ’552 Patent, Defendants direct and aid third parties, including without limitation end-users of the accused products, to infringe the ’552 Patent by, among other things, (i) enabling a user of the accused products to use the products to support the securement of electronic information and its associated cryptographic keys, as claimed in the ’552 Patent; (ii) providing instructions (including, by way of example, software downloads, product demos, technical documents, whitepapers, and other training located at https://bull.com/hardware-security-module-hsm/, https://bull.com/hsm-trustway-proteccio-nethsm/, and https://bull.com/crypt2pay-hsm-cryptographique/) to end-users of the accused

products for using the products in their customary way; (iii) advertising the accused products' support of the securement of electronic information and its associated cryptographic keys; and (iv) providing to third parties the products, software, and related equipment that may be required for or associated with infringement of the '552 Patent, all with knowledge that the induced acts constitute patent infringement. Defendants possess specific intent to encourage infringement by third parties, including without limitation end-users of the accused products. **Exhibit B** includes examples of Defendants' advertisements and instructions to users of the accused products regarding support of the securement of electronic information and its associated cryptographic keys.

Secure storage

The core function is to create and store securely secret keys, private keys are certified public keys. Identifiers and other key attributes are defined through the GUI and saved in the database with encrypted key values. Key partitioning is achieved through the definition of key hierarchies.

Access Control

The connection of KMC application to **crypt2pay** HSM is secured by TLS. The KMC operator is authenticated by **crypt2pay** HSM through the presentation wof a user certificate on a smart card.

Certification Authority

KMC integrates Certification Authority (CA) functions for signing the SSL certificates. This integrated CA can be used to avoid the need of an external PKI solution.

Secret Share

Root keys shall be recovered from key shares introduced by key cus todians to unlock access to the lower level keys in the hierarchy. Key shares can be stored on smart cards for convenience and security.

Trusted path

Introduction of key share values inside the HSM's secured memor y can only be performed through a PIN PAD with direct and secured connection to the HSM.

A printer can be connected to the HSM's serial port to print key shares for backup purposes.

Key Import/Export

Secret keys can be imported or exported through the PIN PAD (key shares) or in encrypted form in XML files. Several encryption mechanisms are supported to import or export secret or private keys using symmetric or asymmetric cryptography.

Scripting feature

Scripting feature can be used to automate key generation and EMV Issuer Certificate Request generation. As a result, productivity of key ceremonies is improved.

Target key stores

Key distribution scheme is defined through the HSM management function. Each target is assigned a list of keys among all keys stored in the database in order to ensure that each target has all the keys it needs for its production, and only the keys it needs. Distribution rules can be defined for single HSMs or groups of HSMs. Key stores are produced for each target with integrity and confidentiality protections. Several key stores format are supported depending on the target HSM vendor and target application.

Report & Audit logs

Each operation is recorded in an audit log file protected in integrity. Customized Key Ceremony reports can be issued to ensure traceability of key management operations.

Meta data

Meta data may be defined and associated with keys to customize the key management to the target environment.

Exhibit B at 2, available at https://bull.com/wp-content/uploads/2016/08/f-kmc-en4_web2.pdf.

INDIRECT INFRINGEMENT (CONTRIBUTION - 35 U.S.C. §§ 271(c) and/or (f))

26. Based on the information presently available to No Magic, No Magic contends that Defendants have indirectly infringed, and continue to indirectly infringe the ’552 Patent, including but not limited to at least one or more of Claim 1, Claim 4, Claim 16, Claim 17, and one or more dependent claims, by contributing to the infringement of the ’552 Patent under 35 U.S.C. § 271(c) and/or 271(f), either literally and/or under the doctrine of equivalents, by selling, offering for sale, and/or importing into the United States, the accused products.

27. The accused products are capable of the securement of electronic information and its associated cryptographic keys. Defendants know that the accused products (i) constitute a material part of the inventions claimed in the ’552 Patent; (ii) are especially made or adapted to infringe the ’552 Patent; (iii) are not staple articles or commodities of commerce suitable for non-infringing use; and (iv) are components used for or in systems that are capable of the securement of electronic information and its associated cryptographic keys as claimed in the ’552 Patent.

28. No Magic is informed and believes that Defendants intend to and will continue to directly and indirectly infringe the ’552 Patent. No Magic has been damaged as a result of Defendants’ infringing conduct described in this Count. Defendants are thus liable to No Magic in an amount that adequately compensates No Magic for its infringement, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

VII. JURY DEMAND

29. Plaintiff No Magic demands a trial by jury of all matters to which it is entitled to trial by jury, pursuant to FED. R. CIV. P. 38.

VIII. PRAYER FOR RELIEF

WHEREFORE, No Magic prays for judgment and seeks relief against Defendants as follows:

A. That the Court determine that one or more claims of the ’552 Patent are infringed by Defendants, either literally or under the doctrine of equivalents;

B. That the Court award damages adequate to compensate No Magic for the patent infringement that has occurred, together with prejudgment and post-judgment interest and costs, and an ongoing royalty for continued infringement;

C. That the Court award such other relief to No Magic as the Court deems just and proper.

DATED: April 7, 2017

Respectfully submitted,

/s/ Eric M. Albritton

Eric M. Albritton
Texas State Bar No. 00790215
ema@emafirm.com
Shawn A. Latchford
Texas State Bar No. 24066603
sal@emafirm.com
ALBRITTON LAW FIRM
111 West Tyler Street
Longview, Texas 75601
Telephone: (903) 757-8449
Facsimile: (903) 758-7397

Andrew G. DiNovo
Texas State Bar No. 00790594
adinovo@dpelaw.com
Jay D. Ellwanger
Texas State Bar No. 24036522
jellwanger@dpelaw.com
Daniel L. Schmid
Texas State Bar No. 24093118
dschmid@dpelaw.com
DiNovo Price Ellwanger & Hardy LLP
7000 North MoPac Expressway
Suite 350
Austin, Texas 78731
(512) 539-2626 (phone)
(512) 539-2627 (fax)

**ATTORNEYS FOR PLAINTIFF
NO MAGIC, INC.**